Common OT Security Misconceptions

mamdouhmuhammad

mamdouh.de

“OT systems are isolated (air-gapped) from IT or the internet.”

Reality:

Modern OT is often connected to corporate networks for monitoring and remote access, making them reachable by attackers.

“Legacy OT systems can’t be hacked.”

Reality:

Older PLCs/RTUs lack authentication and encryption, making them vulnerable even if not originally designed for online use.

“Availability is the only thing that matters.”

Reality:

Integrity (correct process control) and confidentiality (e.g., recipe data) are also critical. Attacks can cause unsafe conditions even when systems stay “up.”

“Standard IT security tools will protect OT just fine.”

Reality:

Traditional antivirus and patching can break fragile OT systems or require downtime plants can’t afford; OT needs tailored security measures.

“Standard IT security tools will protect OT just fine.”

Reality:

Traditional antivirus and patching can break fragile OT systems or require downtime plants can’t afford; OT needs tailored security measures.

“Physical security

=

cybersecurity.”

Reality:

Remote exploits via vendor VPNs, phishing, or infected maintenance laptops can bypass physical barriers.

“Once you set up firewalls, you’re safe.”

Reality:

Misconfigurations, shared credentials, and unmonitored conduits can let attacks pass; security needs monitoring, detection, and layered defenses.